Mýty antivirové ochrany virtuálních a fyzických serverů

Proč organizace hřeší na zabezpečení svých serverů, co je odrazuje od ochrany virtualizovaných strojů, jak vyvrátit falešné mýty administrátorů a jak nasadit účinnou ochranu, vysvětluje René Pospíšil, security solution strategist pro Bitdefender CZ/SK.

Jak z vaší zkušenosti přistupují firmy k zabezpečení serverů před malwarem?
Při diskuzích s partnery a zákazníky hodně narážíme na to, že administrátoři věří mýtu, že servery není potřeba proti malwaru chránit. Hlavním důvodem pro nezabezpečení bývá obava z nadměrného zatížení virtualizovaných strojů.

Administrátoři často buď částečně vypínají funkcionalitu antimalwarových řešení, nebo je vůbec neinstalují s tím, že si myslí, že jim stačí jen dobře konfigurovat firewall a vyškolit obsluhu.

Jak se dá mýtus o nepotřebě zabezpečení serverů vyvrátit?
Nelze se spoléhat na lidský faktor a správné konfigurace serverů. Problémem je, že na server může útočit i někdo z koncového bodu z vnitřní sítě. Například u souborových serverů je otevřená spousta portů, přes které jsou snadno zranitelné.

Navíc samotný operační systém má spoustu zranitelností, a než se objeví záplata, může je útočník využít. Většinou útočníka zajímají data a ta jsou především na serverech. Takže servery je potřeba chránit adekvátní ochranou.

Z čeho pak ale plyne obava, že anti-malware nadměrně zatěžuje virtuální servery?
Platí to zejména ve virtuálním prostředí, kde většina antivirových řešení používá běžného klienta, který využívá zbytečně moc zdrojů a způsobuje tzv. antivirové bouře.

Jednak dochází k mrhání IT zdroji při opakovaném skenování, a tudíž duplikaci skenů, které se pouštějí na každém virtualizovaném stroji a zbytečně skenují již jinde na jiném stroji proskenované identické soubory, a jednak se u těchto zastaralých řešení stahují signatury (typicky ve stejnou dobu několikrát denně) do každého VS nebo VD, takže vzniká zbytečná zátěž na hypervizoru, která mnohdy vede ke zmrazení celého hypervizoru.

Pro virtuální stroje přece existují i speciální verze…
Tradiční výrobci antivirů od 90. let zásadně nezměnili strukturu řešení. Je sice pravda, že spousta výrobců používá pro servery virtualizované skrze VMware jeho rozhraní vShield. To znamená menší zátěž než u klasického klienta, ale skýtá to v sobě nebezpečný kompromis, neboť vShield pro skenování zprostředkovává pouze soubory, a neumožňuje skenování paměti, služeb a registrů.

Další nevýhodou je, že takto lze chránit pouze Windows OS, ale ne Linux či jiné operační systémy. Nelze zajistit vysokou dostupnost, protože vShield umožňuje pouze jeden host driver, a pokud tento spadne, zmizí s ním i skenovací funkcionalita a schopnost virtualizované stroje chránit.

Má tedy ochrana virtuálních serverů nějaké spolehlivé a účinné východisko?
Ano, je ovšem potřeba změnit přístup, opustit tradice a používat inteligentní, na hypervizoru nezávislé klienty, které se nahrají do virtualizovaného prostředí jinak – tak, že fungují jako brána, přes kterou se jen zprostředkovává antimalwarová služba, a samotný skenovací proces pak probíhá na speciálních bezpečnostních appliancích ve vysoké dostupnosti.

Jak lze docílit snížení nákladů na instalaci a následný provoz?
Pokud je řešení postaveno na již předinstalovaných linuxových appliancích, tak není nutné platit za operační systém a ani databázi ne. Další obrovskou výhodou takových řešení je, že šetří čas administrátora – od několika hodin až po několik dnů –, protože odpadá instalace jak OS, tak DB, a dokonce i samotného řešení.

Správce se opravdu soustředí na podstatné, a tím jsou konfigurace produktu i následná správa politik. Ta nejmodernější řešení dovedou navíc také globálně deduplikovat skeny, a to nejen v rámci firemní sítě, ale ideálně i vůči globální bezpečnostní síti v cloudu.

Suma sumarum, takto v kombinaci pak lze oproti tradičním antivirovým řešením řádově uvolnit desítky procent výpočetního výkonu a nemalé částky v pořízení a provozu.

Jaké novinky lze v blízké budoucnosti očekávat?
S ohledem na to, že se množí viry na úrovni hypervizoru a tradiční antivirové řešení nedovedou dostatečně čelit útokům typu APT (Advanced Persistent Threat) a v reálném čase zamezit jejich šíření, lze očekávat vývoj technologií, které se na tuto problematiku budou specializovat.

Takovou první vlaštovkou je HVI neboli Hypervisor „Memory" Introspection, což je řešení, které umožňuje ochránit samotný hypervizor. Díky přímému přístupu přes speciální ovladače do paměti umí udělat bezpečnostní analýzu virtualizovaných strojů, a umožňuje takto detekci a zamezení spuštění bezpečnostních hrozeb nultého dne v reálném čase.

Výhodou je, že toto řešení dovede zablokovat spuštění útočného kódu, například APT, aniž útočník ví, že jeho kód zastavil nějaký bezpečnostní mechanismus zasahující z vyšší úrovně přímo z hypervizoru. Administrátor má tedy vyšší práva než útočník. HVI skýtá zásadní průlom v ochraně virtualizované infrastruktury.